IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION PAPERS OF

LEE CODEL LAWSON TARBOTTON, TREVOR HUGH RICE,

GUY WILLIAM WELCH ROBERTS, ANDREW JOHN PETER BIDGOOD

and CARL STEVEN BOTTERILL

FOR

MECHANISMS FOR BANNING COMPUTER PROGRAMS FROM USE

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to the field of data processing systems. More particularly, this invention relates to mechanisms for banning from use computer programs that may be executed on data processing systems.

Description of the Prior Art

As computer systems and networks become larger, more complex and more critical to the operation of many businesses and institutions, there exists a need to control the computer programs that may be executed on those systems. Generally speaking, there will be a core set of computer programs that are properly intended for execution on a computer system. An individual user may add to this set further computer programs specific to their needs or requirements. There also exists a category of computer programs that it is desired to ban from use on a computer system. Examples of such programs are games and programs that can consume excessive resources, such as data streaming programs.

Whilst it is desirable to provide mechanisms that can enforce the banning of certain computer programs, it is advantageous if these mechanisms do not themselves represent a significant additional overhead in terms of installation, maintenance and consumption of processing resources. To this end, it has been proposed that banned computer programs could be treated as if they were computer viruses and the mechanisms that are already in place upon many computer systems to combat computer viruses be used to enforce the banning undesired, although not actually virus-like, computer programs. Whilst such an approach is superficially attractive as it could effectively prevent execution of unwanted computer programs without requiring an addition system and without consuming significant additional processing resources, it has the disadvantage that there is no universally accepted view of which computer programs should be banned from use. In some organisations, it may be entirely acceptable for games to be executed on computer systems, whilst in other organisations this may be strictly prohibited. Accordingly, the anti-virus computer system provider would need to produce a wide set of banned computer program definition data such that individual users could pick the appropriate definition data to ban their particular set of unwanted computer programs. This would represent an impractical additional overhead on the anti computer virus system provider as a very large number of different banned program definition files would be required. Furthermore, it is undesirable for the anti-computer virus program provider to become involved in deciding which computer programs are potentially of a sort that a user may wish to ban.

SUMMARY OF THE INVENTION

Viewed from one aspect, the present invention provides a computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of one or more computer programs to be banned from use, said computer program comprising:

(i) user controlled program specifying logic operable to specify one or more computer programs to be banned from use; and

(ii) banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said one or more computer programs to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

The invention preserves the desirable characteristics of utilising the - anti-computer virus systems to enforce computer program banning whilst avoiding the disadvantages of requiring the system provider to produce many different banned computer program identifying data types by providing a tool to end users to themselves specify their own collection of computer programs that they wish to ban from their systems. This tool can then be used to generate banned program identifying data that interfaces with and controls an anti computer virus system to take banning measures against those computer programs specified as banned by a particular user.

It will be appreciated that the generation of anti-computer virus definition data relating to banned programs by end users could lead to misuse with malicious persons introducing definition data that treated some essential or desired computer program as banned when this was not intended. In order to help resist this, preferred embodiments of the invention are such that the tool only produces encrypted banned program identifying data using a private key. This encrypted data will only be decrypted into a form where it is usable by computer programs having a corresponding matching public key. Thus, banned computer program identifying data can be made specific to a particular organisation such that will not be effective if it propagates outside of that organisation. Furthermore, unless a set of banned computer program identifying data was produced using the private key corresponding to a particular machine's public key, then that definition data will not operate on the computer with the public key.

The use of an anti-computer virus mechanism for enforcing banning of computer programs has the advantage that such mechanisms already incorporate the provision for heuristic analysis. Accordingly, banned computer program identifying data can incorporate heuristic characteristics of banned computer programs such that new versions of those computer programs that are likely to show similar heuristic characteristics will also be likely to be identified as also being banned.

In a highly secure environment, the system may be utilised to produce banned computer program identifying data that effectively comprises a list of permitted computer programs with all computer not matching that list being treated as banned.

Viewed from another aspect, the present invention provides a computer program product comprising a computer program operable to control a computer to ban from use one or more computer programs, said computer program comprising:

(i) anti computer virus logic responsive to user generated banned program identifying data for said one or more computer programs to be banned from use to identify computer programs banned from use.

As well as providing the tool for generating the appropriate banned program identifying data, the invention also provides a system responsive to that data for enforcing the banning of undesired computer programs.

In order to enhance the security of the system, preferred embodiments may be arranged such that when the banned computer program identifying data is decrypted, it is stored within a secure memory region such that it is more resistant to malicious tampering.

When a banned computer program is identified, various actions may be taken. One or more of the following actions may be desired: issuing an alert message to a user or network administrator indicating identification of a banned computer program, denying access to the banned computer program, encrypting the banned computer program to render it unusable and/or deleting the banned computer program.

Preferred embodiments of the invention may also seek to protect themselves from being circumvented by a user deleting the banned computer program defining data by detecting the absence of this data and performing one or more of: issuing an alert message to the network administrator, restoring the missing data from a remote source or disabling the computer until the missing data is put back in place.

In some embodiments, the banned computer program enforcing mechanism can be implemented using the same instance of anti-virus computer software as is concurrently used for protecting the computer from computer virus threats. However, in other embodiments, it may be desirable to provide a separate concurrently running instance of such an anti-virus system that is solely responsible for the enforcement of banning of certain computer programs.

Other aspects of the invention also provide a method of generating banned program identifying data, a method of banning from use one or more computer programs, apparatus for generating banned program identifying data and apparatus for banning from use one or more computer programs.

BRIEF DESCRIPTION OF DRAWINGS

The above and other objects, features and advantages of the invention will be apparent from the following detailed description of illustrative embodiments which is to be read in connection with the accompanying drawings, in which:

Figure 1 schematically illustrates the relationship between an operating system and an anti-virus system;

Figure 2 is a flow diagram illustrating the operation of the tool for generating banned computer program identifying data;

Figure 3 is a flow diagram illustrating operation of the anti-virus computer system; and

Figure 4 is a diagram schematically illustrating a general purpose computer for forming the above-described techniques.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 illustrates an operating system 2 that co-operates with an anti-virus system 4. In use, file access requests are received by the operating system 2 as a result, for example, of application program use or user commands. A file access request is intercepted before it is serviced by the operating system and information characterising the file access request is passed to the anti-virus software 4. This information can include details such as the file name, the access requester, the location of the computer file requested, etc. The anti-virus software 4 uses this information to trigger an anti-virus engine 6 in conjunction with virus definition data 8 to perform an anti-virus scan of the computer file concerned. Such scans may be performed upon an on-access basis as described above or on an on-demand basis as part of regular thorough scan of an entire system. If the computer file in question passes the anti-virus scan, then a pass signal is returned to the operating system 2 which can then continue to service the file access request using, for example, a hard disk drive 10 storing the computer file.

In addition to the virus scanning operation, the anti-virus engine 6 is also responsive to banned computer program identifying data 12. This banned computer program identifying data 12 can have essentially the same form as the virus definition data 8 and can be generated using techniques similar to those that are used to produce new virus definition data as new viruses are released into the wild. However, in this instance, the banned computer program identifying data is generated by an end user themselves rather than the anti-computer virus system provider. The tools required to identify a particular computer program as being a virus or banned are relatively straightforward and suitable for provision in a generic form as compared to the more complicated and problematic tools that are needed to produce programs to repair computer virus damage and the like.

An advantage of using the anti-virus software 4 to identify banned computer programs is that these systems are set up to use identification mechanisms based upon fundamental characteristic of a computer program such that they may not be readily circumvented by merely renaming a computer program or changing insignificant portions of it. This makes anti-virus systems particularly well suited to enforcing the banning of certain computer programs.

Figure 2 is a flow diagram illustrating the creation of banned computer program identifying data. At step 14, a user specifies the computer programs they wish to ban. The user may do this by collecting together within a certain directory key executable files or DLLs from an undesired computer program. It is usually readily apparent which are the key executable files and other files involved in a particular unwanted computer program. Alternatively, all the files associated with an undesired computer program could be banned.

Once the user has assembled the collection of computer files that they wish to be treated as banned, step 16 is performed to generate a set of banned computer program identifying data that may be utilised by the anti-virus software 4.

It will be appreciated that the anti-virus software 4 as illustrated in Figure 1 may be executed as a single instance of that software or alternatively multiple instances may be executed with one only being responsive to genuine virus definition data and the other being responsive to banned computer program identifying data.

The banned computer program identifying data can look for key executable computer instruction sequences within the computer files concerned or alternatively/additionally identify heuristic behavioural characteristics of that computer program that may be analysed in a manner that provides a degree of protection against variants of that computer program.

Once the banned computer program identifying data has been generated, the user may also associate specific actions to be triggered in response to identification of particular banned computer programs. These actions may include issuing an alert message to the user or the system administrator, denying access to the banned computer program in a manner similar to the way access is denied to a computer virus, encrypting the banned computer program rendering it unusable or possibly deleting the banned computer program. These responses may be set as a policy that is applied to all banned computer programs or alternatively may be individually tailored to each banned computer program.

In order to provide resistance against the system being used maliciously, the banned computer program identifying data is encrypted using the private PGP key of the organisation generating it at step 18. Encrypting the data in this way has the result that only a computer using the corresponding public key will successfully decrypt it so rendering the widespread distribution of malicious banned computer program identifying data file less likely.

At step 20, the banned computer program identifying data file may be distributed to all of the target computers using the mechanisms that are normally employed to distribute virus definition data.

Figure 3 is a flow diagram illustrating operation of the anti-virus software. At step 22, the anti-virus software is started. This will typically take place at boot-up in a system that is permanently running anti-virus software. At step 24, the banned computer program identifying data file is decrypted using the public PGP key stored within the computer in question. At step 26, the decrypted file is authenticated.

Although it is not illustrated, if the decrypted data file is not successfully authenticated, then it will not be used. Furthermore, if the banned computer program identifying data file is not present in a form that can be properly authenticated, then various mechanisms may be triggered in order to resist a user trying to circumvent the banning mechanisms. These triggered mechanisms include issuing an alert message to the system administrator, automatically restoring the missing data file from a remote source or possibly disabling the computer concerned until the missing file is put in place. The options to carry out these tasks can be set up by the system administrator at the time that the anti-virus system is installed and do not all need to be used.

At step 28, the properly authenticated banned computer program identifying data is stored within a secure memory area.

At step 30, the anti-virus system waits until a file access request for scanning is received from the operating system 2.

When a file access request is received, step 32 performs a normal anti-virus scan using the virus definition data 8. If the virus scan is not passed as is detected by step 34, then standard anti-virus action is triggered at step 36 and a fail response is returned to the operating system at step 38.

If the anti-virus scan is passed, then processing proceeds to step 40 at which a scan for banned computer programs is performed. This uses the banned computer program identifying data 12 and the standard anti-virus engine 6. If a banned computer program is detected at step 42, then banned actions 44, such as described above, are triggered and a fail response is returned to the operating system 2 at step 46.

If a banned computer program is not detected at step 42, then a pass response is returned to the operating system 2 by step 48.

The above is described in terms of a system that looks for specified banned computer programs. An alternative approach suitable for high security environments is one in which the user specifies a list of permitted computer programs with all other computer programs being treated as banned. The process illustrated in Figure 2 may then be modified to produce data identifying all permitted computer files. The Figure 3 system is then modified to check for permitted files rather than banned files. If a computer file is not positively identified as a permitted file, then it is treated as banned with a fail response being returned to the operating system when it is scanned to see if it belongs to the permitted list of files.

Figure 3 shows the anti-virus scan taking place before the banned scan, but it will be appreciated these could be performed in the other order.

Figure 4 schematically illustrates a computer 200 of a type that may be used to execute the computer programs described above. The computer 200 includes a central processing unit 202, a random access memory 204, a read-only memory 206, a hard disk drive 208, a display driver 210 and display 212, a user input/output circuit 214, a keyboard 216, a mouse 218 and a network interface circuit 220, all coupled via a common bus 222. In operation, the central processing unit 202 executes computer programs using the random access memory 204 as its working memory. The computer programs may be stored within the read-only memory 206, the hard disk drive 208 or retrieved via the network interface circuit 220 from a remote source. The computer 200 displays the results of its processing activity to the user via the display driver 210 and the display 212. The computer 200 receives control inputs from the user via the user input/output circuit 214, the keyboard 216 and the mouse 218.

The computer program product described above may take the form of a computer program stored within the computer system 200 on the hard disk drive 208, within the random access memory 204, within the read-only memory 206, or downloaded via the network interface circuit 220. The computer program product may also take the form of a recording medium such as a compact disk or floppy disk drive that may be used for distribution purposes. When operating under control of the above described computer program product, the various components of the computer 200 serve to provide the appropriate circuits and logic for carrying out the above described functions and acts. It will be appreciated that the computer 200 illustrated in Figure 4 is merely one example of a type of computer that may execute the computer program product, method and provide the apparatus described above.

Although illustrative embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes and modifications can be effected therein by one skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.